Canada: Information Operations

By Commander Derek Moss, Canadian Navy

Editorial Abstract: Commander Moss notes that information is as important as forces, space, and time on the operational level. Canada's IO definition has taken out references to "influence an adversary's decision makers" implying that Canada can now message target audiences that are not adversaries. He references Canadian Marshall McLuhan, who famously wrote "the medium is the message." Finally, CDR Moss notes that Canada has developed a increasingly accurate "measures of effectiveness" (MOE) paradigm.

Introduction

Information Operations is often talked about in tones that suggest it is a panacea, created as an alternative to kinetic action. It is often performed by a group of staff officers who are, physically and by job description, removed from operators. Many talk about it, but few understand it. Although not entirely PSYOP or Public Affairs, it coordinates and advises on both topics, and many more. This article defines Canadian IO concepts and direction, and offers recommendations for fighting extremists' use of the Internet.

Definition of Information Operations

Until recently, Canada defined information operations as "actions taken in support of national objectives that influence an adversary's decision-makers by affecting other's information and information systems while exploiting and protecting one's own information and information systems and those of our friends and allies." An information operation is a "military advisory and coordinating function that targets and affects information and information systems, human or technical, of approved parties in order to achieve desired effects, while protecting our own and those of our allies."

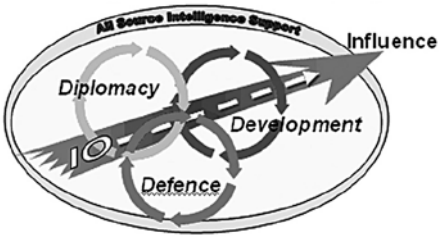
Canada has now removed "influence an adversary's decision-makers" from the definition of information operations. While perhaps only a difference in semantics, the implication of this change may be that we can message target audiences that are not our adversaries. The people of Afghanistan spring to mind. An interesting question would be, "does this target audience include the Canadian public?" From my personal perspective the answer would be yes, even though not formalized in Canadian doctrine. If national opinion is a strategic center of gravity, information operations practitioners had best form relations with the Public Affairs section. Of course this brings to mind the question of whether we are embarking on a slippery slope—though not if all your information is correct, and the Public Affairs Office (PAO) is out front with the message.

With respect to operational art, our opinion is that information now ranks on an equal level with forces, time, and space as the fourth operational factor. It is peculiar because the effects it delivers happen in both the physical and cognitive realms. That particularity has two corollaries: First, only proper targeting and measurement of the effects will allow for a reliable assessment of information activities; Second, the wide range of effects allow for the use of information operations along the full continuum of conflict for both domestic and international operations.

Successful planning, conduct, and execution of operations require that all military and government agencies and organizations involved must cooperate and their activities coordinated. Although the term information operations is defined as a military function, it must be coordinated with other government departments (OGD), or at least be de-conflicted, in order to be successful. Further, information operations "Encompass political, economic, and diplomatic efforts as well as defense and military measures. Coordination among all government departments, under the guidance and direction of the central agencies, is crucial." IO involves the three "Ds" as follows:

Elements of IO

Canada's current IO doctrine is based on original input from 1998, revised in 2004. Now Canada is working closely with NATO to update the latter's doctrine and also with the North American Aerospace Defense Command (NORAD) and US Northern Command (NORTHCOM) IO Staffs. A comparison of US and Canadian IO doctrine as it has developed from 1998 through February 2006 (Figure 1), reveals the following:



Three D's of IO. (Author)

Canada believes that offensive information operations include actions taken to influence an adversary's decision-makers; and these operations may be done by affecting kinetically or non-kinetically an adversary's use of or access to information and information systems. Defensive information operations, from Canada's perspective, include actions taken to protect one's own information and that of one's friends and allies. Defensive IO ensures friendly decision-makers have timely access to necessary, relevant, and accurate information; and ensures that the friendly decision-making process is protected from all adverse effects, deliberate or accidental.

Electronic Warfare (EW) is defined as actions taken to exploit the electromagnetic (EM) spectrum which encompasses the interception and identification of EM emissions. It includes the employment of EM energy, including directed energy, to reduce or prevent hostile use of the EM spectrum and actions to ensure its effective use by friendly forces.

Computer network operations include defensive, offensive, and exploitation activities. Computer network attack (CNA) involves actions taken through the use of computer networks to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves. Computer network defense (CND) involves actions taken through the use of computer networks to protect, monitor, analyze, detect, and respond to unauthorized activity within Department of Defense information systems and computer networks. Computer network exploitation (CNE) enables operations and intelligence collection capabilities conducted through the use of computer networks to gather data from target or adversary automated information systems or networks.

Operations Security is the process which gives a military operation appropriate security, using passive or active means, to deny the enemy knowledge of the dispositions, capabilities, and intentions of friendly forces.

Deception is measures designed to mislead the enemy by manipulation, distortion, or falsification of information, to induce them to react in a manner prejudicial to his interests.

Psychological Operations are planned activities designed to influence attitudes and behaviors, affecting the achievement of political and military objectives.

Civil-Military Cooperation is a military function that supports the commander's mission by establishing and maintaining coordination and cooperation between the military force and civilian actors in the commander's Area of Operations.

Public Affairs is a distinctive function within DND/CF that helps establish and maintain mutual lines of communications, understanding, acceptance, and cooperation between an organization and its audiences.

IO targets include decision-makers, perceptions, information systems, the C4ISR communication infrastructure, software, and data.

Terrorism – the Canadian Context

Canada is facing several terrorist threat elements: religious extremism, with various Sunni Islamic groups being the most serious threat at present; state-sponsored terrorism; secessionist violence, which encompasses Sikh extremism, and separatist movements in Sri Lanka, Turkey, Ireland and the Middle East; and domestic extremism, including some anti-abortion, animal rights, anti-globalization, and environmental groups. Plus there exists a small but receptive audience for militia messages emanating from the United States, white supremacists, and elsewhere.

With the possible exception of the United States, there are more international terrorist organizations active in Canada than anywhere in the world. This situation can be attributed to Canada's proximity to the United States which currently is the principal target of terrorist groups operating internationally; and to the fact that Canada, a country built upon immigration, represents a microcosm of the world. It is therefore not surprising that the world's extremist elements are represented here, along with peace-loving citizens, as part of Diaspora communities.

Most terrorist activities in Canada are in support of actions elsewhere. In recent years, terrorists from different international terrorist organizations have come to Canada posing as refugees. Other activities include:

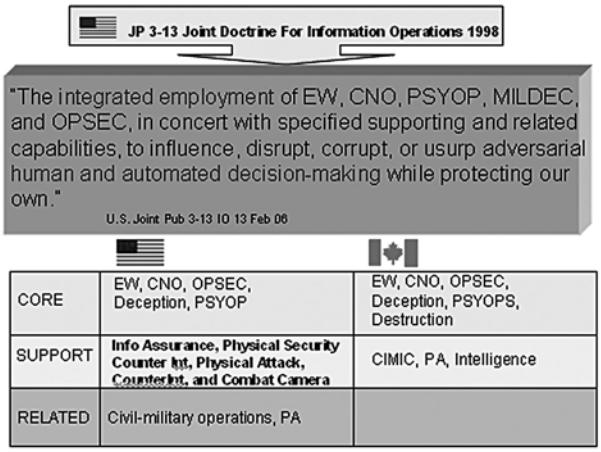


Figure 1. CA & US doctrines compared. (Author)

• Fund-raising and lobbying through front organizations;

• Providing support for terrorist operations in Canada or abroad;

• Procuring weapons and materiel, coercing and manipulating immigrant communities, facilitating transit to and from the United States and other countries, and other illegal activities.

All of these functions are facilitated by the use of the Internet, and remain among the core components of cyber-terrorism.

One of the sponsoring registrars for Hizballah is Register.com located in New York (but with offices in many places). The municipality and province provided hundreds of thousands of dollars in perks to convince it to locate operations in Yarmouth, (southeastern) Canada. And, it has a very specific policy for dealing with cases where someone reports a domain being used for illegal purposes.

"This policy includes reviewing the content to determine the validity of the report and, if applicable, disabling the domain and notifying the customer of the reason for this action," says Wendy Kennedy, the firm's manager of public relations and customer marketing. "At times, Register.com has also reached out to law enforcement to report suspicious activity."

But the servers in Yarmouth are by no means the only ones in Canada where terrorist-related content may be residing. Until a few weeks ago, the website for Al Qaeda in the Islamic Maghreb, one of the most extensive and regularly updated of its kind, was registered to a building near downtown Toronto. The address belongs to Contactprivacy, the anonymous-registration arm of Canadian domain-name provider Tucows Inc. After its Web-hosting service in Germany was alerted to the Maghreb site and pulled the plug earlier this year, Tucows followed suit. But in an environment where similar sites are popping up daily, it was a small victory.

Porn versus Terror

Years ago, authorities noticed that child pornography websites, though often operated from outside North America, made use of North American anonymous-registration services. In response, a large number of watchdog groups began hunting down such sites to force the registration firms to shut them down. Wade Deisman, Director of the National Security Working Group near the University of Ottawa, noted in August 2007 that "There's nothing near that level [of public monitoring] with terrorist websites" and "I haven't seen anything that comes even close to addressing this issue." If you shut down a terrorist site, you still can't arrest it's originator. If you keep it going, you can at least monitor the site.

Countering Terrorist Use of the Internet

Terrorist use of the Internet can be countered when a terrorist attack is computer based; is orchestrated by a foreign government, terrorist group, or politically motivated extremists; or is done for purposes of espionage, sabotage, foreign influence, or politically motivated violence. Ward Elcock, Canadian Security Intelligence Service (CSIS) Director to the National Joint Committee of Senior Criminal Justice Officials, noted on 22 November 2001 that "Our role is to determine what is out there so as to provide adequate warning to government and, where appropriate, to law enforcement agencies about threats to the security of Canada, in particular from terrorism. If we lose our ability to do so, then Canadians and our allies will have been ill served." The threat of attacks on critical information systems and the infrastructures that depend on them will, in the foreseeable future, be almost impossible to eliminate entirely, owing to the fact that attack tools, networks, and network control systems are constantly evolving. As new technologies develop, so too will new attack tools along with the sophistication of the perpetrators who use them.

The Canadian Cyber Incident Response Center (CCIRC) is the national focal point for addressing cyber security issues. A component of the government operations center, it is located under the national emergency response system. CCIRC is the focal point for reporting real or imminent threats and incidents. It includes a threats and vulnerability identification and analysis, early warning dissemination, and incident strategic response and coordination elements.

Protecting Canada's telecommunications networks is a job too big and too important for any one company or government. Therefore:

• A partnership approach to cyber security provides the momentum, speed, and flexibility required to address emergencies and the challenges presented by emerging technologies;

Dominion of Canada (Wikimedia)

• Industry Canada, as the lead government department for telecommunications, has established the Canadian Telecommunications Cyber Protection Working Group (CTCP) to promote industry-to-industry, government-to-industry, and industry-to-government cooperation in protecting Canadian networks;

• Industry Canada and the CTCP Working Group have established the Canadian Network for Security Information Exchange (CNSIE) to promote collaboration among larger communities of cyber security stakeholders such as the telecommunications, financial, energy, and vendor communities and other government departments;

• Collaboration has been established with domestic and international partners such as the Canadian Cyber Incident Response Center (CCIRC), as well as the US and UK Network Security Information Exchanges.

Short-term Solutions

Two agencies, the Royal Canadian Mounted Police (RCMP) and CSIS, are lead counterterrorism elements in Canada. They have access to a wide range of investigative tools and powers —including physical surveillance, interception of communications (telephone, computer, pager, etc.), and recruitment of human sources or agents who can report on suspects' activities and intentions. Legislation, ministerial directions, and policy define what can be investigated and which tools can be used under what circumstances. Many powers require prior ministerial and judicial authorization. In addition, both agencies are subject to independent review.

Just because an investigative capability is lawful and available does not mean it will be used automatically. Canadian intelligence and law enforcement agencies do not have the human and technological resources to target all potential targets all the time. For the most part, they focus on two categories—first, leaders and principal organizers and second, those who represent a serious threat in that they are known to have engaged in terrorist activity in the past or are believed to be planning future terrorist action in Canada or abroad.

Investigations involving targets residing, working, or hiding in Diaspora communities may present serious challenges. Police and intelligence agencies may not possess the requisite linguistic skills, or may be unable to penetrate closely-knit groups using human sources or agents. They may

face resistance to requests for community cooperation, may fail in attempts to recruit new officers from within the community, and may even be unable to find individuals prepared to work as translators. They may be forced to take extraordinary measures to protect the identity of agents or employees who fear for their safety in closely-knit Diaspora communities. Such measures may include:

• Joint investigations involving Canadian and foreign police or intelligence agencies. Terrorist global connections and movements call for global cooperation to track them and prevent them from taking violent actions. CSIS has reported that it has cooperation arrangements with about 230 agencies in about 130 countries, while many foreign police and security agencies have permanent liaison staff in Canada.

• Designation of individuals or entities associated with terrorist activity. Canada did adopt a designation process for terrorists, terrorist groups, or state sponsors of terrorism after 11 September. By October 2003, the Canadian list included 31 organizations—10 each based in the Middle East and Asia, four based in South America, three in Africa, and one in Europe.

• Security screening of applications for refugee or permanent resident status or for Canadian citizenship. If terrorism links surface during background checks, the government may commence deportation action. Additionally, the Canadian Government can expel suspected terrorists under special security provisions of the Immigration Act, and has done so more than a dozen times.

• Screening of people and goods at ports of entry. Transport Canada, Immigration and Citizenship Canada, the Canada Customs and Revenue Agency, and other organizations have enhanced their screening for terrorist connections since 11 September. A new agency, the Canadian Air Transport Security Agency, performs this role at Canadian airports.

Long-term Solution

Canadian security and intelligence agencies seek to build positive counter-terrorism relationships with some Diaspora leaders and groups in the following ways:

• Consultations and briefings on policy or legislative proposals (for example, those affecting changes in immigration/refugee criteria or charity regulations);

• Membership on advisory boards (the RCMP Commissioner's Multicultural Advisory Committee, for example);

• Community liaison with police officers assigned to specific Diaspora communities to raise awareness, increase confidence, and promote open cooperation with Canadian authorities;

• Direct requests for help and cooperation, usually through community leaders or associations (such as the Canadian Arab Federation) and in connection with specific events (for example, visits to Canada by controversial foreign leaders) or in relation to specific investigations.

Change: Information Operations in Operations

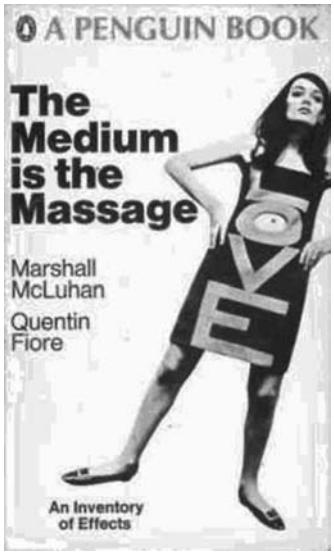
It wouldn't be a Canadian article without a shameless reference to a famous native son. (William Shatner, Mike Myers, John Candy, or any other Hollywood hack will not be quoted.) Instead, the reference here is to Marshall McLuhan (see book jacket), a name endured by many Canadians during painful undergrad classes.

One of McLuhan's lesser known books (pictured), is strangely prescient. Although not prescriptive, the book's thesis, broadly speaking, is that historical changes in communications and craft media change human consciousness, and that modern electronics are bringing humanity full circle to an industrial analogue of tribal mentality, what he termed "the global village." By erasing borders and dissolving information boundaries, electronic telecommunications are fated to render traditional social structures like the nation state and the university irrelevant.

McLuhan's book was written in 1967 yet it has a lasting premise. Shortly we'll discuss how we apply it today. But first we need to explore an earlier work, *Understanding Media: The Extensions of Man,* source of McLuhan's most famous quote:

In a culture like ours, long accustomed to splitting and dividing all things as a means of control, it is sometimes a bit of a shock to be reminded that, in operational and practical fact, the medium is the message. This is merely to say that the personal and social consequences of any medium—that is, of any extension of ourselves—result from the new scale that is introduced into our affairs by each extension of ourselves, or by any new technology.

Two examples highlight changes introduced by technology. First, *Rana FM* is a Canadian Forces radio station broadcasting in Afghanistan but located



in Kingston, Ontario (two hours outside of Toronto). The broadcast is recorded on-site and digitally transmitted via satellite. Rana FM uses an effective listener feedback capability, the only one in the area of operations. Callers to the station, whether by phone or text message, call a local Afghanistan number and have their message recorded to an in-theatre digital repository. This message is stored and quickly forwarded to Kingston and put on the air, with only a 0.6 second delay. Rana has demonstrated its potential to be a giant campaign-winning enabler with its interactive nature since Operation Athena on 6 January 2007. Rana can be

heard in Kandahar City, the Kandahar Airfield region, in Sperwan Ghar and, shortly, in Spin Boldak (but spare parts are scarce).

Second, *My Thum* is a cell phone aggregator that also develops applications for automated responses (SMS, voice, or the Internet) to cell calls or Internet contacts. *My Thum* services the radio industry in the Toronto area. It works by accessing all of the local cell phone carriers, and setting up a system that aggregates these carriers with one number (an SMS "short code" which is simply an easily remembered six digit number that callers can recall and dial from any cell system). The short code automatically brings any cell carrier user/customer to an automated response that is either voice or SMS in the case of cell phones (or the Internet if so desired). The caller is guaranteed a response.

Commercially, *My Thum* is used mainly for contests and have great utility for "polling the audience" safely and inexpensively. The automated response can and usually is set to automatically answer and offer an 'invitation' to join the station's 'club' to receive early advisories on programs, contests, etc. Because the law in Canada requires users to agree to receive SMS from 'businesses,' this automated system invites them to join, thus agreeing to receive whatever messages are sent to them.

Measures of Effectiveness (MOE)

MOE are developed as part of the planning process to determine the effects of IO activities. MOE must link our IO coordinated activities (cause) to the response generated by adversarial capabilities and decision makers.

The initial objectives set the course, but MOE act as the rudder in order to maintain that course. MOE feedback allows IO planners the ability to revise, create, and delete IO objectives and themes as required, in order to support the commander's mission. Regardless of its importance, the conduct of a MOE has been largely overlooked. Within Canada, we have developed such a system and have used it successfully in two missions (Operations Halo and Athena). J3 Information Operations leads the MOE effort by developing a combination of quantitative or objective questions and qualitative or subjective questions that are felt to accurately reflect the information needed to establish whether an objective is being met. These questions are then distributed to appropriate stakeholders such as Canada's Assistant Deputy Minister for Policy, PA, intelligence and those in theatre. Once the answers are received they are compiled by the J3 Information Operations staff and are then assigned a value of "met, partially met, or not met" to each objective. The final product is sent back to the contributing stakeholders to seek agreement on the assessment.

Conclusions

Overall, Canada has a very robust telecommunications industry which, through close collaboration with the government, is able to mitigate many cyber attacks against communication networks. As an example, the recent attacks against Estonia, which caused a significant stir and amounted to not much more than a national five-day inconvenience, would have caused a five minute disruption in Canada. This has nothing to do with advanced technology. In fact, Estonia is one of the most communications-advanced countries in the world. Canadian successes are the result of a vested interest in the telecommunications industry in maintaining a robust system based on redundant technologies and no single points-of-failure. Short-term technological solutions will be an ongoing, iterative process until longer-term social solutions are found. Long-term solutions will not eliminate the problem, but they will make it more manageable.